Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Николаев Дмитрий Иванович, НПМмд-02-24

Содержание

# 1 Цель работы

Изучить работу алгоритмов дискретного логарифмирования в конечном поле — -метод Полларда для дискретного логарифмирования, а также реализовать его программно.

# 2 Теоретическое введение

## 2.1 Дискретное логарифмирование в конечном поле

Задача дискретного логарифмирования, как и задача разложения на множители, применяется во многих алгоритмах криптографии с открытым ключом. Предложенная в 1976 году У. Диффи и М. Хеллманом для установления сеансового ключа, эта задача послужила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулевым разглашением и других криптографических протоколов.

Пусть над некоторым множеством произвольной природы определены операции сложения «+» и умножения «». Множество называется *кольцом*, если выполняются следующие условия:

1. Сложение коммутативно: для любых ;
2. Сложение ассоциативно: для любых ;
3. Существует нулевой элемент , такой, что для любого ;
4. Для каждого элемента существует противоположный элемент , такой, что ;
5. Умножение дистрибутивно относительно сложения:

для любых .

Если в кольце умножение коммутативно: для любых , то кольцо называется *коммутативным*.

Если в кольце умножение ассоциативно: для любых , то кольцо называется *ассоциативным*.

Если в кольце существует единичный элемент такой, что для любого , то кольцо называется кольцом с единицей (или *унитарным*).

Если в ассоциативном, коммутативном кольце с единицей (АКУ-кольце) для каждого ненулевого элемента существует обратный элемент , такой, что , то кольцо называется *полем*.

Пусть , . Целые числа и называются *сравнимыми по модулю*  (обозначается ), если разность делится на . Некоторые свойства отношения сравнимости:

1. *Рефлексивность*: .
2. *Симметричность*: если , то .
3. *Транзитивность*: если и , то .

Отношение, обладающее свойством рефлексивности, симметричности и транзитивности, называется отношением *эквивалентности*. Отношение сравнимости является отношением эквивалентности на множестве целых чисел.

Отношение эквивалентности разбивает множество, на котором оно определено, на *классы эквивалентности*. Любые два класса эквивалентности либо не пересекаются, либо совпадают.

Классы эквивалентности, определяемые отношением сравнимости, называются *классами вычетов по модулю* . Класс вычетов, содержащий число , обозначается или и представляет собой множество чисел вида , где ; число называется представителем этого класса вычетов.

Множество классов вычетов по модулю обозначается , состоит ровно из элементов и относительно операций сложения и умножения является *кольцом классов вычетов* по модулю .

Пример. Если , то , где - множество всех четных чисел, - множество всех нечетных чисел.

Обозначим , где - простое целое число, и назовем конечным полем из элементов. Задача дискретного логарифмирования в конечном поле формулируется так: для данных целых чисел и , , , найти логарифм - такое целое число , что (если такое число существует). По аналогии с вещественными числами используется обозначение .

Безопасность соответствующих криптосистем основана на том, что, зная числа , вычислить легко, а решить задачу дискретного логарифмирования трудно. Рассмотрим -Метод Полларда, который можно применить и для задач дискретного логарифмирования. При этом случайное отображение должно обладать не только сжимающими свойствами, но и вычислимостью логарифма (логарифм числа можно выразить через неизвестный логарифм и ). Для дискретного логарифмирования в качестве случайного отображения чаще всего используются ветвящиеся отображения, например:

При имеем , а при имеем

## 2.2 Алгоритм, реализующий -Метод Полларда для задач дискретного логарифмирования

**Вход**. Простое число , число порядка по модулю , целое число , ; отображение , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

**Выход**. Показатель , для которого , если такой показатель существует.

1. Выбрать произвольные целые числа и положить , .
2. Выполнять , , вычисляя при этом логарифмы для и как линейные функции от по модулю , до получения равенства .
3. Приравняв логарифмы для и , вычислить логарифм решением сравнения по модулю . Результат: или “Решений нет”.

### 2.2.1 Пример

Решим задачу дискретного логарифмирования , используя -Метод Полларда. Порядок числа 10 по модулю 107 равен 53.

Выберем отображение при , при . Пусть , . Результаты вычислений запишем в таблицу:

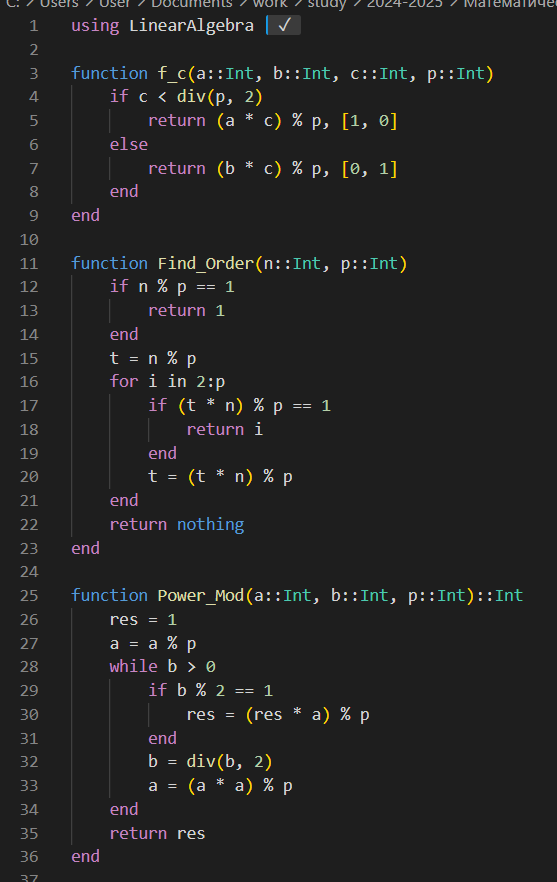
Приравниваем логарифмы, полученные на 11-м шаге: . Решая сравнение первой степени, получаем: .

Проверка: .

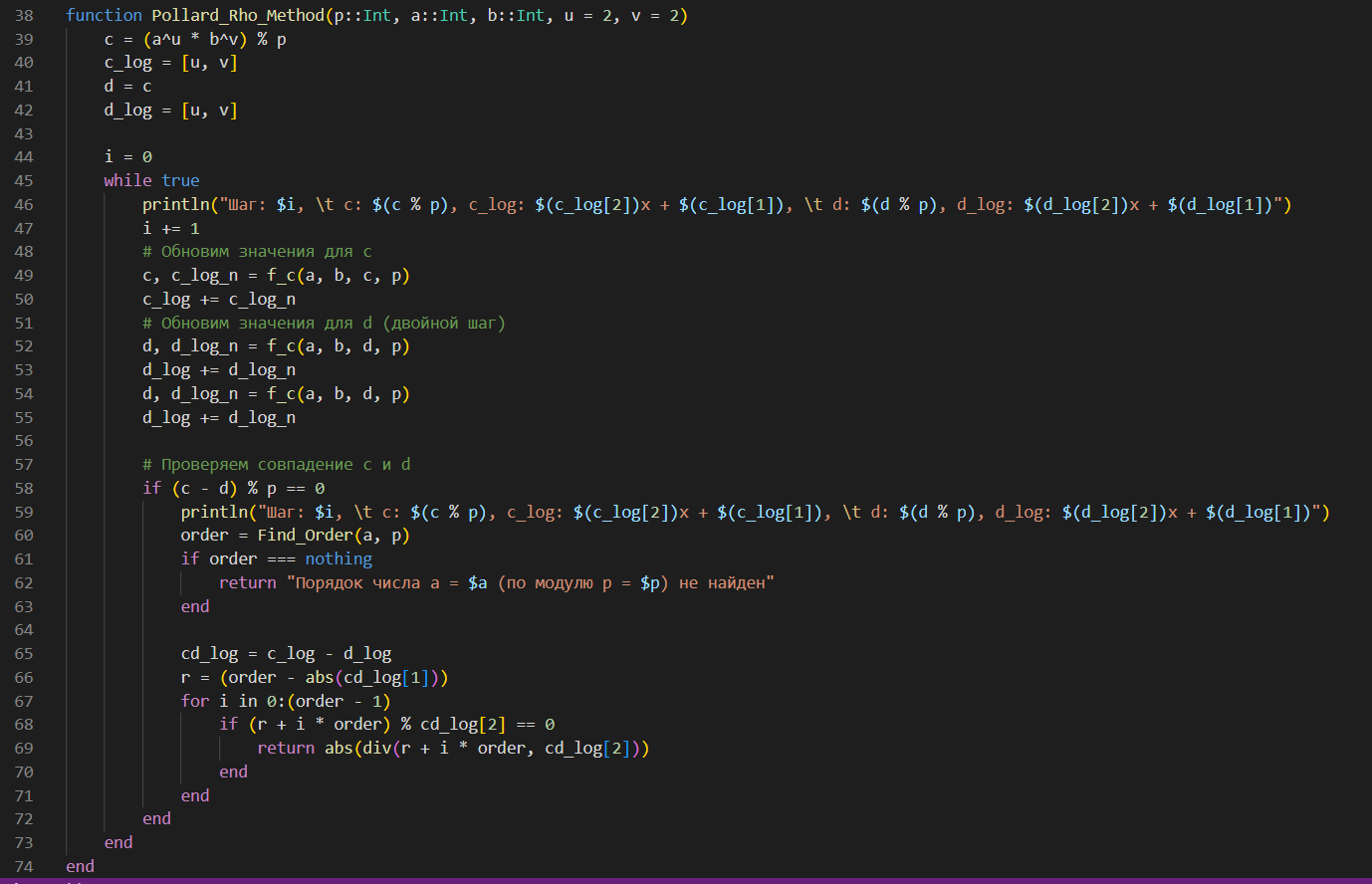
# 3 Выполнение лабораторной работы

Действуя согласно [1], реализуем все описанные алгоритмы на языке Julia.

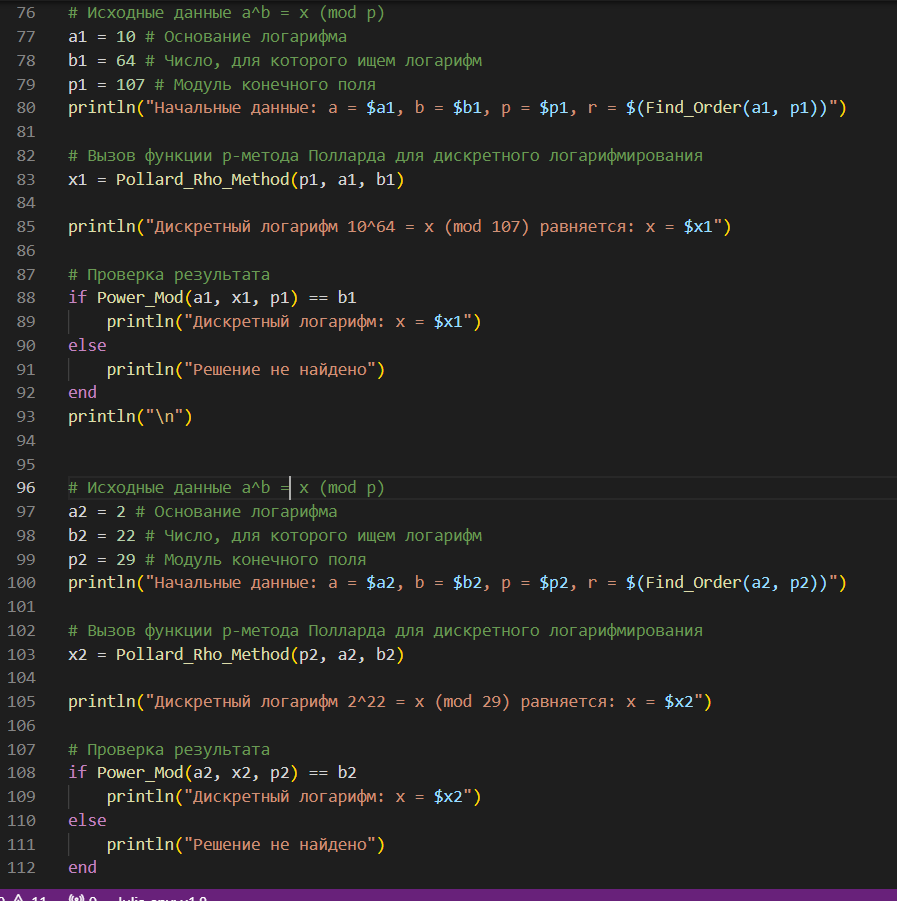
Сначала реализуем несколько функций (Рис.[??]): функцию, обладающую сжимающими свойствами; функцию по нахождению порядка числа в конечном поле, и функцию модульного экспоненциирования. Далее реализуем функцию -метода Полларда для нахождения дискретного логарифма (Рис.[??]). После чего найдём дискретный логарифм для двух случаев: , (Рис.[??]); в результате чего получим следующий вывод, представленный на Рис.[??].



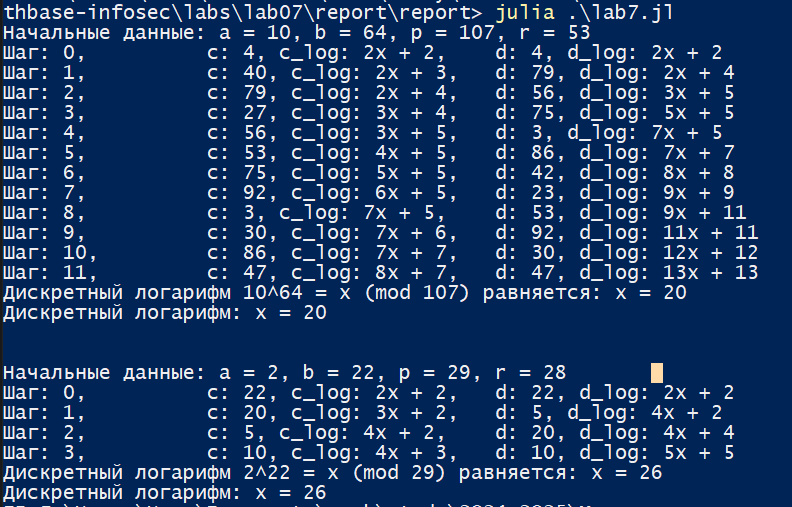
Код вспомогательных функций на Julia



Код алгоритма -Метода Полларда для дискретного логарифмирования на Julia



Начальные данные для нахождения дискретного логарифма на Julia



Результат выполнения кода по решению задачи дискретного логарифмирования на Julia

# 4 Выводы

В ходе выполнения лабораторной работы я изучил работу алгоритмов дискретного логарифмирования в конечном поле — -метода Полларда для дискретного логарифмирования, а также реализовал его программно.

# Список литературы

1. Лабораторная работа № 7. Дискретное логарифмирование в конечном поле [Электронный ресурс]. Саратовский государственный университет имени Н.Г. Чернышевского, 2024.